METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATION NETWORK

The invention relates to a method for accessing a service in a telecommunication network, ~~be it~~ which may be a private network, an intelligent network or a mobile radio ~~network~~ ~~proceeding~~ from an arbitrary communication terminal device, ~~wherein it is necessary~~ to authenticate oneself by ~~means of~~ entering digit sequences in order to receive access to a desired service. ~~Besides~~ In addition, the invention relates to a device in a telecommunication network, which makes it possible to carry out a secure authentication of a user in the case of a service call.

Description of the Related Art

Given an intelligent network IN, an architecture is concerned that makes it possible, in a communication network, to offer services to users of this network. These what are ~~referred to as~~ value-added services give network operators the opportunity to differentiate themselves from competitors and to develop additional income sources.

In order to be able to offer value-added services, the network operator needs at least one central node in his network (service control point), which ~~has the~~ stores bits of information ~~stored~~ that are necessary for ~~purposes of~~ carrying out the services (e.g., storing the service programs, forwarding to responsible network nodes etc.). This central node is also referred to as implementing entity.

The users in such a communication network can ~~thereby~~ utilize interesting new services. One of the better known services is the ~~what is referred to as~~ 'credit card calling' service, in which the ~~calling~~. The caller is ~~hereby~~ charged via his credit card with the fees for actuated calls. Apart form

Such an access protection is also imaginable regarding other services, for example, for users in a mobile network, a private network or a private virtual network.

In all these cases, the authenticating digit code is entered via the keyboard of the terminal device and is transparently (i.e., in plaintext) transmitted via the lines and switching nodes of the communication network.

There are two possibilities to ~~spy out~~ inappropriately acquire these access codes:

a) by ~~spying out~~ acquiring the PIN, be it by observing the authorized user ~~with respect to the input~~ entering it via the keyboard of his terminal device, ~~also~~ or by video monitoring;

b) by tapping the PIN with respect to the transmission between terminal device and the performing entity.

SUMMARY OF THE INVENTION

The invention is based on the object of proposing a possibility as to how the access to services in a telecommunication network can be fashioned more secure.

This object is achieved by means of a method according to patent claim 1.

The utilized method describes the following course of action:

~~the~~ An unambiguous digit sequence for securing the access is encoded subsequent to ~~the~~ an input by ~~means~~ way of an encoding function or a mathematical one-way function, which are known to someone skilled in the art.

A one-way function is a mathematical function f(x) = y, ~~whereby~~ in which y is simple to calculate; ~~vice versa~~ from x; however, the determination of x from y, on the other hand, is extremely complex and not necessarily unambiguous.

A further parameter is co-encoded, which changes with each new input of the digit sequence. Therefore, each new encoding process supplies a new result.

Together with the variable parameter, this result is subsequently coded directly per protocol or is coded into a digit sequence, and is sent in multi-frequency signaling potentially via switching nodes up to the central entity.

The transmission ensues in the same way as the previous process of the authentication.

Then, the central entity evaluates the transmitted digit sequence in that a result is also calculated from the known one-way function using the expected PIN and the co-supplied parameters and is compared to the ~~in the [sic]~~ received value.

The realization of this authentication method is comparatively simple. A sufficient number of encoding methods are known to someone skilled in the art. The implementation of the method is only necessary on the side of the user and at the central entity; the implementation expenditure ~~outlay~~ is low. An ~~already present~~ already-present data bank can be simply expanded by a field for storing the already received access codes.

The advantage of the described method clearly lies in the protection of the user. The expenditure ~~outlay~~ is not greater for the user than in previous methods, since they also required entry of an access code ~~previously had to be entered as well~~. However, an unauthorized user is efficiently prevented from calling at the expense of others. ~~This misuse is hitherto~~ Misuse is possible, since it is not a precondition that the user also has the credit card when he enters the credit card number, for example. Thus, the access could be gained in a simple way by ~~means of~~ simply observing the entered number including PIN.

~~In this case, the~~ But with the inventive method lacking knowledge about the utilized encoding method additionally prevents ~~from the~~ unauthorized usage.

The access code is fashioned such that it is secure against tapping; one or more variable parameters are added, such as a specification about the point in time of the

request. ~~Thereby, a tapping trial~~ in the network (for example on the access line) becomes useless, since a repeatedly used access code is rejected in the first place.

~~This object is achieved by means of a device according to patent claim 9.~~

A device for purposes of encoding the entered PIN is ~~thereby~~ utilized. This device requires an input device (keyboard) similar to the one ~~of~~ the communication terminal device. The device converts the entered digit sequence by ~~means~~ of the mathematical one-way function, together with a variable parameter. Together with the second parameter, the result of the calculation is subsequently translated into multi-frequency signaling methods and is transmitted to the terminal device.

The transmission up to the central entity ensues from there.

The central entity carries out an authentication with the received access code.

In addition to the previously cited advantages, a critical advantage of ~~this course of action~~ is the possibility of being able to ~~already~~ enter the ~~number a longer period of~~ time before the actual usage. Thus, at least the 'spying-out' by means of observing the input of the number can be effectively prevented.

Advantageous embodiments and developments are provided in the subclaims.

The inventive course of action is particularly advantageous with respect to specific ~~works~~ of telecommunication networks. First of all, the architecture of the intelligent network is to be ~~named, wherein~~, for example, the service 'credit card calling' has already been implemented. The infrastructure required for the method is already present. Apart from the private networks, which require a mechanism for accesses from outside, there is also the VPN - the 'Virtual Private Network', which is realized in IN technology as well. Finally, the method is also ~~imaginable~~ in communication

networks for mobile radio telephone service; ~~here~~, the user must authenticate himself for a device as well.

A plurality of possibilities are imaginable for the variable parameters. In the most simple case, a random number is created each time; corresponding generator functions for random numbers are known to someone skilled in the art.

Another possibility is a time specification, for example a dividing in a time-slot pattern of arbitrary nature. ~~In this case~~, the central entity, ~~on one hand~~, can check whether the received access code is a current value. ~~Further~~, the additional transmission of the variable parameter is potentially not necessary when the transmitter and the receiver are ~~synchronized otherwise~~ in terms of time.

Another possibility is the generation of a mathematical progression with an initial number n, ~~whereby~~ the sequence number n2 can result from its precursor number n1 in different ways, such as summing ~~up~~ a fixed ~~value~~.

Numerous methods and functions are known to someone skilled in the art regarding the type of encoding. In particular, the ITU recommendation X.509 and the RFC 1938 represent different complex and secure authentication and encoding methods.

The ITU recommendation X.509 particulary represents two methods.
The first and more simple method only uses an encoding process. The one-way function f is applied to one or more variable parameters and the PIN, possibly expanded by a string that is known to the ~~MFV~~ transmitter and the telecommunication service. The result from f (parameter1, [parameter2, ...], PIN) is converted into a digit string, which is then transmitted by ~~means~~ of the MFV transmitter.

It is more complex to realize a two-step encoding ~~and it~~ also requires more computing power with respect to the transmitter and receiver; however, ~~it~~ also offers a significantly higher protection.

In two step encoding, a

A ~~A~~ first encoding step ~~thereby ensues~~ occurs in the same way as the above cited, single-step
A method. Subsequently, a second pass occur with a second mathematical algorithm f' (which can be identical with the first function f); the result calculates as follows:
f' (parameter x1 [,parameter x2, ..], f (parameter y1 [,parameter y2], PIN), PIN.

A generalized encoding process requires the multiple application of one algorithm or of different algorithms, respectively with the input parameters PIN and additional variable parameters.

When the result of the encoding is not a numeric digit sequence, or when the result
A cannot be transmitted without ~~MVF [sic]~~ MFV tones (as it is the case with respect to ISDN), the result must be translated in such a digit sequence prior to the transmission.

A The authentication method checks the transmitted digit code which determines ~~. It is thereby detected~~
A whether the user is authorized to access a service. It can ~~be~~ additionally determine ~~detected~~ whether the digit code that is authorized to access a service is misused.

The authentication can proceed as follows:

- The central entity checks whether the sent access code has already been
A received once in a fixed time interval, and if so,
A ~~When this is the case~~ the authentication is discontinued as unsuccessful.
- A ~~In the other case~~ Otherwise, the central entity calculates the access code to be
A expected by ~~means~~ way of the same one-way function and the second parameter contained in the received access code and compares the result to the received one. The authentication is successful when the calculated and received code match. The user is allowed to access the desired service.

It can be advantageous to integrate the encoding device into the communication
A terminal device ~~. Thus,~~ so that the user does not have a second device that can get lost.

Transmission errors of the encoding device to the terminal device are also avoided. A generator for MFV tones, which is already present in the terminal device, can be utilized and potentially modified.

The application possibilities of this method in a telecommunication network (particularly an intelligent network, a private network or a mobile network) are versatile. Particularly ~~the~~ a fee aspect represents a critical factor not only for the service provider but also for the network user.

~~In particular, the~~ Particularly credit card telephony is associated with an extremely high risk, ~~Particularly~~ especially since the extent of the damage does not become obvious before the next invoice, since a loss of the card is not noticed in the case of misuse.

Both sides can achieve an extremely high advantage with a comparatively small ~~outlay~~ expenditure.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is subsequently explained on the basis of exemplary embodiments. ~~Shown are~~

Figure 1 is a block diagram showing the generation, transmission and authentication of a one-time-access code in an intelligent network,

Figure 2 is a block diagram showing the generation of the one-time-access code according to the ITU X.509, single-step method, and

Figure 3 is a block diagram showing the generation of the one-time-access code according to the ITU X.509, two-step method.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows the path of an access key (PIN) from a user up to a central entity (SCP) in an intelligent network.

Subsequent to the input in a device for purposes of encoding (MFV), the PIN is transmitted ~~by means~~ via of dial tones to the terminal device (KE) and from there is transmitted into the communication network to the central entity (SCP). ~~En route, switching centers (SSP) are passed via which the encoded access code is currently~~

service control point

INSAIS> ~~transparently transmitted. The access code could hereby be spied out by means of~~ at this point ~~tapping~~. The central entity (SCP) checks the access code on the basis of already known data, for example, from a data bank (DB), and the co-supplied data from the supplied digit string. After the expected access code ~~to be expected~~ has been calculated and compared to the received one, an acknowledgment message is created which reflects ~~made [sic]~~ thus whether or not the transmitted access code is correct and the user is allowed access ~~as a result thereof~~.

Figure 2 and Figure 3 schematically show the generation of an access code that is to be transmitted via the network to the central entity. A symmetrical key is ~~thereby~~ required (PIN), which is known to the user and the central entity, which carries out an authentication. The PIN itself is not transmitted in a decoded manner.

In addition, two variable parameters may be co-encoded ~~are co-encoded here~~ - a time specification (time, time') and a random number. These components change with each authentication process and thus prevent a detected one-time-access code from being used again. When these components cannot be automatically derived with respect to the central entity, they must be co-transmitted during the authentication.

Additional data, such as ~~an~~ arbitrary text, can also be utilized for the formation of the one-time-access code. These data are either known to both sides or are derivable or are additionally transmitted.

An encoded access code (rpPIN) is generated by way ~~means~~ of the one-way function f (and f').

AID

Bibliography

ITU-T x.509
Information Technology - Open Systems Interconnection -
The Directory: Authentication Framework
ITU-T Recommendation x.509, 11/93

RFC 1938
Request for comments: 1938, May 1996
A one-time password system
N. Haller, Bellcore, C. Metz, Kaman Sciences Corporation

Abbreviation list

f, f'	mathematical functions
IN	intelligent network
ITU	international telecommunication union
KE	communication terminal device
MFV	multi-frequency method
PIN	personal identification number
rpPIN	replayprotected [sic]PIN
SCP	service control point
SSP	service switching point